Havells India

Security Exception Management Policy

Version 1.0

Document Approvers

S. No.	Type of Information	Document Data
1.	Document Title	Havells India Security Exception Management Policy
2.	Document Code	HSEMP
3.	Date of Release	20th Feb 2023
4.	Document Superseded	
5.	Document Approvers	Mr. Pramod Mundra and Mr. Ramanand Jha
6.	Document Owner	Information Security Head
7.	Documents Author(s)	Mr. Sanjay Roongta and Mr. Neeraj Nagpal

Document Approvers

S. No.	Approver	Approver Designation	Approver Contact
1.	Pramod Mundra	Chief Information Officer (CIO)	Pramod.Mundra@havells.com
2.	Ramanand Jha	Information Security Head (ISH)	ramanand.jha@havells.com

Document Change Approvals

Version No	Revision Date	Nature of Change	Date Approved
1.0	NA	Initial Version	18th Feb 2022
1.0	NA	No change	17th Feb 2023

Document Scope

This document shall be applicable to the IT Department and the employees/Third Parties referred henceforth shall include the staff working with IT department and/or handling, processing, and managing information/information assets of Havells.

Document Distribution

The Information Security Head (ISH) shall distribute this policy to all employees working with IT department and/or handling, processing, and managing information/information assets of Havells by uploading it on the intranet/by sharing it via email/as appropriate.

Document Conventions

All statements in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the policy.

Table of Contents

1. Purpose

The purpose of this policy is to describe the Security Exception Management Policy within the context of steady state delivery of services and to ensure continuous functioning of business processes while safeguarding the information/information assets involved from information security related threats and risks.

1.1 Scope

This policy shall be applicable to the IT department and the employees/Third Party who deal with Havells' IT and/or handle, process or manage information/information assets of Havells.

1.2 Responsibility

It is the responsibility of the IT Team, Security team and respective or concerned business/functional team to implement and maintain the guidelines as defined in the Security Exception Management Policy.

1.3 Enforcement

All employees and/or third party, who deal with Havells' IT and/or handle, process or manage information/information assets of Havells, must comply with this policy. All statements in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the policy.

Non-compliance with this policy shall be dealt with in accordance with the approved management process.

a) Employees and third party who breach this policy shall be subject to disciplinary action;

b) In case of third parties, appropriate clauses incorporated in the contract / agreement for violations / non-compliances of policy shall be invoked as per the specified process.

1.4 Authority

The Chief Information Officer (CIO) and Information Security Head (ISH) approves and enforces this policy and mandates processes to monitor and ensure compliance to this policy.

2. Policy

This document specifies the process for Exception Document (ED) creation, implementation & maintenance. The Exception Document management process enables systematic documentation (online portal / workflow / paper based) of residual business risk accepted by the information asset owner. Such residual risk is recognized & documented ((online portal / workflow / paper based) by this process after it is deemed necessary to allow exception Havells Information Security Policy provisions due to technical feasibility and/or business cost justification.

Some examples that Exception Process includes:

a) Removable storage media, CDs, USB storage devices will be allowed only after approval;

b) Installation and usage of trial or evaluation software on end user machine;

c) Admin rights on end user machine;

d) Patch not being applied in due period to be allowed only after the approval from IT Team.

2.1 List of policies

<table>
<tr><th>Policy No.</th><th>Policy Statement</th><th>Related Documents</th></tr>
<tr><td>2.1.1</td><td>Exception should be identifiable by a unique tracking /exception ID</td><td></td></tr>
<tr><td>2.1.2</td><td>Authorized requesters:
Havells' employees are considered as valid Exception requesters. Third party can raise Exception by routing request through Havells' employees. As there is no concept of permanent Exception & the Exceptions which will get renewed for more than 3 quarter period will be sent to Havells Information Security Team for evaluation for inclusion in relevant policy documents.
Types of valid security exception requests are:
<table>
<tr><th>ED Type</th><th>Risk Attached</th><th>Vulnerability</th></tr>
<tr><td>Proxy Removal (direct Internet Access)</td><td>High</td><td>Vulnerabilities associated with proxy may be exploited;</td></tr>
<tr><td>Access Control
Examples:
1) Admin Access on Server
2) Email Access on Personal PCs
3) Internet Access
4) Local Admin Access on Laptop/Desktop
5) USB Access
6) VPN Access
7) Website Access Approval
8) Wi-fi Access</td><td>High</td><td>Unauthorized access control can lead to access for sensitive information. So, permission should be given very carefully;</td></tr>
</table></td><td></td></tr>
</table>

Policy No.	Policy Statement			Related Documents
	Removal of DLP client	High	Removal of DLP client may allow leakage of sensitive data to unauthorized person & outside agencies which would directly impact business;	
	Other exceptions	Depending upon the exception type	Unauthorized access or vulnerabilities associated with exception can result in compromise of confidentiality, integrity and availability of Havells' information /information assets /information processing facilities.	
2.1.3	Retaining of evidence Designated personnel from Security team/IT team shall be responsible for approving the Exception request according to the business need. Exception records shall be centrally maintained. This will allow easier retrieval for audit review.			
2.1.4	Receiving of Exception requests Exception requests can be created on central exception portal & approved by designated personnel from Security team/IT team.			Exception Portal
2.1.5	Dashboard dashboard shall contain all Exception details including Business Approver, IT Approver, unique tracking/exception number.			ED Dashboard

2.2 Roles and Responsibilities

Role	Organization	Responsibility
Requester	Business team /Third Party vendor	Requester is defined as user from Business team/ third-party vendor of Havells requesting exception w.r.t Information Security Policy and underlying policy/process for a valid business reason. Requester shall be responsible for below responsibilities such as: a) Request of relevant Exception by properly mentioning the details ; b) Requestor to contact Local Helpdesk or IT team/Security team for filling of Exception details on / via email/ITSM

<table>
<tr><th>Role</th><th>Organization</th><th>Responsibility</th></tr>
<tr><td>Requester ’s Manager / Business Function Head, Tech lead and CIO /ISH</td><td>IT team /Security team /Business team</td><td>Business team and tech lead shall be responsible for approving Exception post analysing that the request has a proper business justification, risk acceptance and mitigations. Request can be approved over email/ ITSM tool
Approval Matrix
<table>
<tr><th colspan="3">Approving Authority</th></tr>
<tr><td>Organization</td><td>Requestor’s Manager / Business Function Head</td><td>Tech lead / CIO/ ISH</td></tr>
<tr><td rowspan="2">Havells India</td><td>Y</td><td>Y</td></tr>
<tr><td>Y</td><td>Y</td></tr>
<tr><td rowspan="2">Third Party</td><td>Y</td><td>Y</td></tr>
<tr><td>Y</td><td>Y</td></tr>
</table>
</td></tr>
</table>